

iovation ReputationManager™

Protect your business and your customers with device reputation. By adding iovation ReputationManager™ to your fraud management process, you'll gain powerful advantages in your battle against fraud and abuse.

Overview

Reduce Fraud Losses and Boost Profitability

Fraud and abuse erode your hard-earned revenue—especially when you're dealing with repeat offenders and organized fraud rings. With iovation, you can immediately identify the size and scope of a problem, shut down all accounts related to a problem, and prevent bad computers from creating more accounts. Plus, iovation alerts you to suspicious behavior so you can take action before you're hit. You'll be surprised how quickly the service starts positively impacting your bottom line.

Gain Operational Efficiencies

Time is money. Cut down on your operational expenses by placing iovation at the beginning of your fraud management process. Streamline your workflow by having the information you need to make fast, confident decisions. You'll increase the automation of your process and zero in on transactions that most need review. We guarantee you'll get more done in less time, with fewer resources.

Maximize Consumer Confidence

Fraud prevention isn't all about the bad guys. It is also about ensuring that your good customers have a positive, hassle-free experience. Device reputation ensures you'll have a safe and secure site, without resorting to strict policies and restrictions that inconvenience the end-user and limit your ability to do business. The result is a fraud protection service that actually contributes to the acquisition, retention, and loyalty of your good customers.

FRAUD AND ABUSE TYPES

Not all types of bad behavior are the same. That's why iovation provides over 30 unique fraud and abuse categories that enable you to differentiate between types of bad devices. Evidence types include:

- CHARGEBACKS
- IDENTITY THEFT
- AFFILIATE FRAUD
- HARASSMENT
- SPAM
- SOLICITATIONS
- ACCOUNT TAKEOVERS

“

iovation has been nothing short of a miracle. They've created what is, in my opinion, the very best third-party anti-fraud system out there.

John Kothanek
Director of Risk Operations,
OBOPAY

”

TOP FEATURES



Real-Time Responses to Reputation Queries

When a device is interacting with your business—at account creation, site login, checkout, or any other point on your site—you send a query to iovation's database in order to instantly find out if that device has already been associated with fraud or abuse. This real-time response allows you to automatically allow, deny, or review transactions and make decisions with an incredibly low false-positive rate.

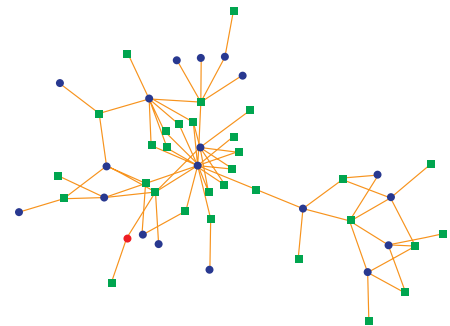
*** REAL-TIME RESPONSE ***

result: D - deny request
reason: - evidence exists



Global Network of Associations

With access to the world's largest database of device intelligence, you benefit from information gathered from billions of transactions across multiple industries. You will be able to uncover relationships between accounts and devices within your own network and also be alerted when you see a device that has already been associated with negative behavior at another subscriber site. iovation continually analyzes the information in our vast database to provide you with the most relevant data and identify patterns and indicators of suspicious activity.



Customized Business Rules

Business rules allow you to identify computers exhibiting behaviors that you find suspicious. You can establish customized velocity thresholds—such as how many accounts you will allow to be created or accessed from one device—and evidence-based rules that identify accounts or devices associated to specific evidence types placed by you or another subscriber. When an account or device triggers a velocity threshold or an evidence-based rule, iovation will return a “deny” or “review” response, and you can decide how to handle the transaction.

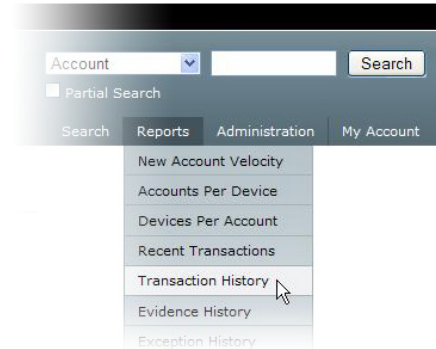
Status	Reason
ALLOW	trusted accounts
DENIED	device exceeds 4 accounts
DENIED	device exceeds 4 accounts
DENIED	trusted evidence
REVIEW	other subscriber evidence
REVIEW	other subscriber evidence
REVIEW	other subscriber evidence
REVIEW	max acct's created per wor



Research & Reporting

The web-based administrative console is used to manage and research information about the accounts and devices on your site. You can submit evidence of fraud that you have encountered, conduct further research on issues you have already identified, and run ad-hoc reports. iovation also offers custom daily reports that can be delivered directly to you through e-mail. Use the admin to:

- Place fact-based evidence
- Handle exception cases
- Generate on-demand reports
- Search your accounts and devices
- View account to device relationships
- Identify suspicious activity



Powerful Risk Scoring for New Devices

iovation Risk Module, a popular add-on to iovation ReputationManager, helps assess the potential risk of devices that are new to the iovation network. Every transaction that comes from a new device will be assigned a risk score based on the presence of specific device characteristics and/or similarities to known fraudulent devices. This gives you the ability to proactively review suspicious behavior.

<input checked="" type="checkbox"/>	Device Profile
<input checked="" type="checkbox"/>	JavaScript Disabled
<input checked="" type="checkbox"/>	Time Zone Mismatch
<input checked="" type="checkbox"/>	Anonymous Proxy
<input checked="" type="checkbox"/>	IP Address

Fight Fraud with Device Reputation

No matter what tools make up your current fraud prevention process, adding iovation ReputationManager will help you significantly minimize fraud loss, gain operational efficiencies, and enhance your customer acquisition and retention strategies.

To learn more about using iovation ReputationManager to protect your business from fraud and abuse, visit www.iovation.com or call 503.224.6010 today.